1. A method for securing data in a computer system having at least a data input device, a processor and memory, all interconnected together, said memory having distributed segments, comprising:

establishing a group of security sensitive words, characters or icons;

filtering data input from said data input device and extracting said security sensitive words, characters or icons from said data to obtain extracted data and remainder data;

separately storing said extracted data and said remainder data in different distributed memory segments; and,

permitting reconstruction of said data via said extracted data and remainder data only in the presence of a predetermined security clearance.

2. A method as claimed in claim 1 wherein the establishing step includes identifying one or more words, characters, images or icons as security sensitive words, characters or icons.

3. A method as claimed in claim 1 including establishing a plurality of security levels each with a respective security clearance, the step of establishing said security sensitive words, characters or icons including correlating said plurality of security levels with subsets of said security sensitive words, characters or icons and the step of permitting reconstruction including the step of permitting a plurality of partial reconstructions of said data in the presence of respective ones of said plurality of security clearance levels.

4. A method as claimed in claim 1 including the step of encrypting one or both of said extracted data and remainder data.

5. A method as claimed in claim 4 including the step of encrypting during the filtering step and prior to the storing step.

6. A method as claimed in claim 5 including the step of decrypting during the reconstruction step.

7. A method as claimed in claim 1 including one of destroying or storing said filter after the filtering step.

8. A method as claimed in claim 1 wherein said computer system includes a display fed from video memory having a plurality of frame memory segments, the reconstruction step including interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments.

9. A method as claimed in claim 1 wherein said computer system includes a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces coupled to said processor and said memory, the step of reconstruction including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays.

10. A method as claimed in claim 1 including deleting said data input from said data input device after the step of storing.

11. A method as claimed in claim 1 including mapping said different distributed memory segments.

12. A method as claimed in claim 10 including mapping said different distributed memory segments.

13. A method as claimed in claim 2 including establishing a plurality of security levels each with a respective security clearance, the step of establishing said security sensitive words, characters or icons including correlating said plurality of security levels with subsets of said security

sensitive words, characters or icons and the step of permitting reconstruction including the step of permitting a plurality of partial reconstructions of said data in the presence of respective ones of said plurality of security clearance levels.

14. A method as claimed in claim 13 including the step of encrypting one or both of said extracted data and remainder data.

15. A method as claimed in claim 14 including the step of encrypting during the filtering step and prior to the storing step.

16. A method as claimed in claim 15 including the step of decrypting during the reconstruction step.

17. A method as claimed in claim 16 including one of destroying or storing said filter after the filtering step.

18. A method as claimed in claim 17 wherein said computer system includes a display fed from video memory having a plurality of frame memory segments, the reconstruction step including interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments.

19. A method as claimed in claim 18 including deleting said data input from said data input device after the step of storing.

20. A method as claimed in claim 19 including mapping said different distributed memory segments.

21. A method as claimed in claim 20 wherein the step mapping includes generating and storing one or more maps to said different distributed memory segments.

22. A method as claimed in claim 17 wherein said computer system includes a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces coupled to said processor and said memory, the step of reconstruction including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays.

23. A method as claimed in claim 22 including deleting said data input from said data input device after the step of storing.

24. A method as claimed in claim 23 including mapping said different distributed memory segments.

25. A method as claimed in claim 24 wherein the step of mapping includes generating and storing one or more maps to said different distributed memory segments.

26. A method as claimed in claim 17 including deleting said data input from said data input device after the step of storing.

27. A method as claimed in claim 26 including mapping said different distributed memory segments.

28. A method as claimed in claim 27 wherein the step of mapping includes generating and storing one or more maps to said different distributed memory segments.

29. A method as claimed in claim 1 wherein said computer system is a personal computer and said memory includes fixed drive memory, floppy drive memory and disc drive memory and the method includes identifying distributed segments in one or more of said fixed drive memory, floppy drive memory and disc drive memory.

30. A method as claimed in claim 29 wherein the step of identifying occurs prior to the step of filtering.

31. A method as claimed in claim 28 wherein said computer system is a personal computer and said memory includes fixed drive memory, floppy drive memory and disc drive memory and the method includes identifying distributed segments in one or more of said fixed drive memory, floppy drive memory and disc drive memory.

32. A method as claimed in claim 31 wherein the step of identifying occurs prior to the step of filtering.

33. A method as claimed in claim 1 wherein said computer system includes a plurality of personal computers (PCs) networked together, each PC having distributed memory segments therein, the step of storing including storing one or both of said extracted data and remainder data in respective ones of said PCs.

34. A method as claimed in claim 28 wherein said computer system includes a plurality of personal computers (PCs) networked together, each PC having distributed memory segments therein, the step of storing including storing one or both of said extracted data and remainder data in respective ones of said PCs.

35. A method for securing data in a computer system with one or more security sensitive words, characters or icons, said computer system having at least a data input device, a processor and memory, all interconnected together, said memory having distributed segments, comprising:

filtering data input from said data input device and extracting said security sensitive words, characters or icons from said data to obtain extracted data and remainder data;

separately storing said extracted data and said remainder data in different distributed memory segments; and,

permitting reconstruction of said data via said extracted data and remainder data only in the presence of a predetermined security clearance.

36. A method as claimed in claim 35 including establishing a plurality of security levels each with a respective security clearance, the step of establishing said security sensitive words, characters or icons including correlating said plurality of security levels with subsets of said security sensitive words, characters or icons and the step of permitting reconstruction including the step of permitting a plurality of partial reconstructions of said data in the presence of respective ones of said plurality of security clearance levels.

37. A method as claimed in claim 35 including the step of encrypting one or both of said extracted data and remainder data.

38. A method as claimed in claim 37 including the step of encrypting during the filtering step and prior to the storing step.

39. A method as claimed in claim 38 including the step of decrypting during the reconstruction step.

40. A method as claimed in claim 35 including one of destroying or storing said filter after the filtering step.

41. A method as claimed in claim 35 wherein said computer system includes a display fed from video memory having a plurality of frame memory segments, the reconstruction step including interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments.

42. A method as claimed in claim 35 wherein said computer system includes a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces coupled to said processor and said memory, the step of reconstruction including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays.

43. A method as claimed in claim 35 including deleting said data input from said data input device after the step of storing.

44. A method as claimed in claim 35 including mapping said different distributed memory segments.

45. A method as claimed in claim 43 including mapping said different distributed memory segments.

46. A method as claimed in claim 35 wherein said computer system is a personal computer and said memory includes fixed drive memory, floppy drive memory and disc drive memory and the method includes identifying distributed segments in one or more of said fixed drive memory, floppy drive memory and disc drive memory.

47. A method as claimed in claim 46 wherein the step of identifying occurs prior to the step of filtering.

48. A method for securing data in a computer network having a plurality of computers interconnected together, one of said plurality of computers designated as a data input computer and each of said plurality of computers having a memory therein, a first and a second memory designated as a remainder store and an extract store in one or more computers of said plurality of computers, comprising:

establishing a group of security sensitive words, characters or icons;

filtering data input from said data input computer and extracting said security sensitive words, characters or icons from said data to obtain extracted data and remainder data;

storing said extracted data and said remainder data in said extracted store and said remainder store, respectively; and,

permitting reconstruction of said data via said extracted data and remainder data only in the presence of a predetermined security clearance.

49. A method as claimed in claim 48 including defining a filter prior to said filtering step.

50. A method as claimed in claim 49 wherein the step of defining the filter includes the step of establishing said group of security sensitive words, characters or icons and the method includes one of storing said filter or destroying said filter after storing said extracted data.

51. A method as claimed in claim 48 including encrypting one or both of said extracted data and remainder data prior to storing.

52. A method as claimed in claim 51 wherein the step of permitting reconstruction includes decrypting one or both of said extracted data and remainder data.

53. A method as claimed in claim 48 including establishing a plurality of security levels each with a respective security clearance, the step of establishing said security sensitive words. characters or icons including correlating said plurality of security levels with subsets of said security sensitive words, characters or icons and the step of permitting reconstruction including the step of permitting a plurality of partial reconstructions of said data in the presence of respective ones of said plurality of security clearance levels.

54. A method as claimed in claim 49 wherein one of first and second computers are designated by a uniform resource locator (URL) and said storing utilizes said URLs for said first and second computers.

55. A method as claimed in claim 49 wherein said second computer is designated by a uniform resource locator (URL) and said data input computer operates as a client in a client-server environment wherein said second computer operates as a server, the method including sending said extracted data from said data input computer to said second computer utilizing said URL and client-server protocol.

56. A method as claimed in claim 55 wherein said step of permitting reconstruction includes downloading said extracted data from said second computer utilizing said URL and said client-server protocol.

57. A method as claimed in claim 49 wherein said first and second computers are designated by respective uniform resource locators (URLs) and said data input computer operates as a client in a client-server environment wherein said first and second computers operate as respective servers, the method including sending said remainder data and extracted data respectively from said data input computer to said first and second computers utilizing corresponding URLs and client-server protocols.

58. A method as claimed in claim 57 wherein said step of permitting reconstruction includes downloading said remainder data and extracted data respectively from said first and second computers utilizing corresponding URLs and client-server protocols.

59. A method as claimed in claim 58 including the step of encrypting and decrypting said remainder data and extracted data during sending and downloading.

60. A method as claimed in claim 49 wherein one of said computers includes a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces, the step of reconstruction including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays.

61. A method as claimed in claim 49 including deleting said data input from said data input computer after the step of storing.

62. A method as claimed in claim 49 including mapping said first and second memory.

63. A method for securing data in a computer network with one or more security sensitive words, characters or icons, said computer network having a plurality of computers interconnected together, one of said plurality of computers designated as a data input computer and each of said plurality of computers having a memory therein, a first and a second memory designated as a remainder store and an extract store in one or more computers of said plurality of computers, comprising:

filtering data input from said data input computer and extracting said security sensitive words, characters or icons from said data to obtain extracted data and remainder data;

storing said extracted data and said remainder data in said extracted store and said remainder store, respectively; and,

permitting reconstruction of said data via said extracted data and remainder data only in the presence of a predetermined security clearance.

64. A method as claimed in claim 63 including defining a filter prior to said filtering step.

65. A method as claimed in claim 64 wherein the step of defining the filter includes the step of establishing a group of security sensitive words, characters or icons and the method includes one of storing said filter or destroying said filter after storing said extracted data.

66. A method as claimed in claim 63 including encrypting one or both of said extracted data and remainder data prior to storing.

67. A method as claimed in claim 66 wherein the step of permitting reconstruction includes decrypting one or both of said extracted data and remainder data.

68. A method as claimed in claim 64 including establishing a plurality of security levels each with a respective security clearance, said security sensitive words. characters or icons being correlated with said plurality of security levels with subsets of said security sensitive words, characters or icons and the step of permitting reconstruction including the step of permitting a plurality of partial reconstructions of said data in the presence of respective ones of said plurality of security clearance levels.

69. A method as claimed in claim 64 wherein one of first and second computers are designated by a uniform resource locator (URL) and said storing utilizes said URLs for said first and second computers.

70. A method as claimed in claim 64 wherein said second computer is designated by a uniform resource locator (URL) and said data input computer operates as a client in a client-server environment wherein said second computer operates as a server, the method including sending said extracted data from said data input computer to said second computer utilizing said URL and client-server protocol.

71. A method as claimed in claim 70 wherein said step of permitting reconstruction includes downloading said extracted data from said second computer utilizing said URL and said client-server protocol.

72. A method as claimed in claim 64 wherein said first and second computers are designated by respective uniform resource locators (URLs) and said data input computer operates as a client in a client-server environment wherein said first and second computers operate as respective servers, the method including sending said remainder data and extracted data respectively from said data input computer to said first and second computers utilizing corresponding URLs and client-server protocols.

73. A method as claimed in claim 72 wherein said step of permitting reconstruction includes downloading said remainder data and extracted data respectively from said first and second computers utilizing corresponding URLs and client-server protocols.

74. A method as claimed in claim 73 including the step of encrypting and decrypting said remainder data and extracted data during sending and downloading.

75. A method as claimed in claim 64 wherein one of said computers includes a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces, the step of reconstruction including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays.

76. A method as claimed in claim 64 including deleting said data input from said data input computer after the step of storing.

77. A method as claimed in claim 64 including mapping said first and second memory.

78. A method for securing data in a computer network having a plurality of computers interconnected together, one of said plurality of computers designated as a data input computer, each of said plurality of computers having a memory therein, said plurality of computers including a first and a second designated computer therein, comprising:

establishing a group of security sensitive words, characters or icons;

filtering data input from said data input computer and extracting said security sensitive words, characters or icons from said data to obtain extracted data and remainder data;

designating memory in said first computer as an extract store and designating memory in said second computer as a remainder store;

storing said extracted data and said remainder data in said extracted store and said remainder store, respectively; and,

permitting reconstruction of said data via said extracted data and remainder data only in the presence of a predetermined security clearance.

79. A method as claimed in claim 78 wherein said step of designating includes storing a map of the designated memory.

80. A method as claimed in claim 79 including storing said map in said data input computer.

81. A method as claimed in claim 80 wherein the step of storing said map includes encrypting said map and the step of permitting reconstruction includes the step of decrypting said map.

82. A method as claimed in claim 78 wherein said second computer is said data input computer and the step of filtering occurs thereat.

83. A method as claimed in claim 78 including the step of encrypting one or both of said extracted data and remainder data.

84. A method as claimed in claim 83 including the step of encrypting during the filtering step and prior to the storing step.

85. A method as claimed in claim 84 including the step of decrypting during the reconstruction step.

86. A method as claimed in claim 78 including one of destroying or storing said filter after the filtering step.

87. A method as claimed in claim 78 wherein one of said computers includes a display fed from video memory having a plurality of frame memory segments, the reconstruction step including interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments on said one computer.

88. A method as claimed in claim 78 wherein one of said computers includes a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces, the step of reconstruction including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays on said one computer.

89. A method as claimed in claim 78 including deleting said data input from said data input computer after the step of storing.

90. A method for securing data in a computer network with one or more security sensitive words, characters or icons, said computer network having a plurality of computers interconnected together, one of said plurality of computers designated as a data input computer, each of said

plurality of computers having a memory therein, said plurality of computers including a first and a second designated computer therein, comprising:

filtering data input from said data input computer and extracting said security sensitive words, characters or icons from said data to obtain extracted data and remainder data;

designating memory in said first computer as an extract store and designating memory in said second computer as a remainder store;

storing said extracted data and said remainder data in said extracted store and said remainder store, respectively; and,

permitting reconstruction of said data via said extracted data and remainder data only in the presence of a predetermined security clearance.

91. A method as claimed in claim 90 wherein said step of designating includes storing a map of the designated memory.

92. A method as claimed in claim 91 including storing said map in said data input computer.

93. A method as claimed in claim 92 wherein the step of storing said map includes encrypting said map and the step of permitting reconstruction includes the step of decrypting said map.

94. A method as claimed in claim 90 wherein said second computer is said data input computer and the step of filtering occurs thereat.

95. A method as claimed in claim 90 including the step of encrypting one or both of said extracted data and remainder data.

96. A method as claimed in claim 95 including the step of encrypting during the filtering step and prior to the storing step.

97. A method as claimed in claim 96 including the step of decrypting during the reconstruction step.

98. A method as claimed in claim 90 including one of destroying or storing said filter after the filtering step.

99. A method as claimed in claim 90 wherein one of said computers includes a display fed from video memory having a plurality of frame memory segments, the reconstruction step including interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments on said one computer.

100. A method as claimed in claim 90 wherein one of said computers includes a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces, the step of reconstruction including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays on said one computer.

101. A method as claimed in claim 90 including deleting said data input from said data input computer after the step of storing.

102. A method of securing data having a group of security sensitive words, characters or icons, the method deployed in a client-server computer system with at least one server computer operatively coupled to at least one client computer over a communications network comprising:

accepting data input which includes some words, characters or icons from said group of security sensitive words, characters or icons via said client computer;

filtering said data input and extracting said security sensitive words, characters or icons from said data to obtain extracted data and remainder data;

separately storing said extracted data from said remainder data in one or both of said client computer and server computer; and,

permitting reconstruction of said data via said extracted data and remainder data only in the presence of a predetermined security clearance on said client computer.

103. A method as claimed in claim 102 wherein the step of filtering occurs at one of said client computer and said server computer.

104. A method as claimed in claim 102 wherein one or more of the steps of filtering and separately storing occur at said server computer.

105. A method as claimed in claim 102 wherein said server computer utilizes at least two memory stores and the step of separately storing includes the step of said server computer separately storing said extracted data and said remainder data in respective ones of said two memory stores.

106. A method as claimed in claim 105 including storing a map of said two memory stores.

107. A method as claimed in claim 106 including encrypting at least one of said extracted data prior to storage, said remainder data prior to storage, and said map prior to storage.

108. A method as claimed in claim 107 wherein said map is stored on one of said client computer and said server computer.

109. A method as claimed in claim 108 including the step of decrypting said at least one of said extracted data prior to reconstruction, said remainder data prior to reconstruction, and said map prior to reconstruction.

110. A method as claimed in claim 102 including establishing said group of security sensitive words, characters or icons.

111. A method as claimed in claim 110 including establishing a plurality of security levels each with a respective security clearance, the step of establishing said security sensitive words, characters or icons including correlating said plurality of security levels with subsets of said security sensitive words, characters or icons and the step of permitting reconstruction including the step of permitting a plurality of partial reconstructions of said data in the presence of respective ones of said plurality of security clearance levels.

112. A method as claimed in claim 102 including one of destroying or storing the filter after the filtering step.

113. A method as claimed in claim 102 wherein said computer system includes an output client computer having a display fed from video memory having a plurality of frame memory segments, the reconstruction step including interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments of said output client computer.

114. A method as claimed in claim 102 wherein said computer system includes an output client computer having a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces, the step of reconstruction including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays of said output client computer.

115. A method as claimed in claim 102 including deleting said data input after the step of storing.

116. A method as claimed in claim 102 including mapping the storage of said extracted data and said remainder data in one or both of said client computer and said server computer.

117. A method of securing data from a data input, said data input having one or more security sensitive words, characters or icons, the method deployed in a client-server computer system with at least one server computer operatively coupled to at least one client computer accepting data input over a communications network comprising:

filtering said data input and extracting said security sensitive words, characters or icons from said data to obtain extracted data and remainder data;

separately storing said extracted data from said remainder data in one or both of said client computer and server computer; and,

permitting reconstruction of said data via said extracted data and remainder data only in the presence of a predetermined security clearance on said client computer.

118. A method as claimed in claim 117 wherein the step of filtering occurs at one of said client computer and said server computer.

117. A method as claimed in claim 117 wherein one or more of the steps of filtering and separately storing occur at said server computer.

120. A method as claimed in claim 117 wherein said server computer utilizes at least two memory stores and the step of separately storing includes the step of said server computer separately storing said extracted data and said remainder data in respective ones of said two memory stores.

121. A method as claimed in claim 120 including storing a map of said two memory stores.

122. A method as claimed in claim 121 including encrypting at least one of said extracted data prior to storage, said remainder data prior to storage, and said map prior to storage.

123. A method as claimed in claim 122 wherein said map is stored on one of said client computer and said server computer.

124. A method as claimed in claim 123 including the step of decrypting said at least one of said extracted data prior to reconstruction, said remainder data prior to reconstruction, and said map prior to reconstruction.

125. A method as claimed in claim 117 including establishing a group of security sensitive words, characters or icons.

126. A method as claimed in claim 125 including establishing a plurality of security levels each with a respective security clearance, the step of establishing said security sensitive words, characters or icons including correlating said plurality of security levels with subsets of said security sensitive words, characters or icons and the step of permitting reconstruction including the step of permitting a plurality of partial reconstructions of said data in the presence of respective ones of said plurality of security clearance levels.

127. A method as claimed in claim 117 including one of destroying or storing the filter after the filtering step.

128. A method as claimed in claim 117 wherein said computer system includes an output client computer having a display fed from video memory having a plurality of frame memory segments, the reconstruction step including interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments of said output client computer.

129. A method as claimed in claim 117 wherein said computer system includes an output client computer having a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces, the step of reconstruction including displaying said

extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays of said output client computer.

130. A method as claimed in claim 117 including deleting said data input after the step of storing.

131. A method as claimed in claim 117 including mapping the storage of said extracted data and said remainder data in one or both of said client computer and said server computer.

132. A method of securing data having a group of security sensitive words, characters or icons, the method deployed in a server-client computer system with at least one server computer operatively coupled to at least one client computer over a communications network, said client computer accepting data input which includes some words, characters or icons from said group of security sensitive words, characters or icons, and filtering said data input and extracting said security sensitive words, characters or icons from said data to obtain extracted data and remainder data thereat, comprising:

separately storing said extracted data from said remainder data via server computer; and,

permitting reconstruction of said data via said extracted data and remainder data only in the presence of a predetermined security clearance via said server computer and as adapted to be downloaded to said client computer.

133. A method as claimed in claim 132 wherein said server computer utilizes at least two memory stores and the step of separately storing includes the step of said server computer separately storing said extracted data and said remainder data in respective ones of said two memory stores.

134. A method as claimed in claim 133 including storing a map of said two memory stores.

135. A method as claimed in claim 134 including encrypting at least one of said extracted data prior to storage, said remainder data prior to storage, and said map prior to storage.

136. A method as claimed in claim 135 wherein said map is stored via said server computer.

137. A method as claimed in claim 135 including the step of decrypting via said server computer said at least one of said extracted data prior to reconstruction, said remainder data prior to reconstruction, and said map prior to reconstruction.

138. A method of securing data having a group of security sensitive words, characters or icons, the method deployed in a server-client computer system with at least one server computer operatively coupled to at least one client computer over a communications network, said client computer accepting data input which includes some words, characters or icons from said group of security sensitive words, characters or icons, comprising:

filtering said data input and extracting said security sensitive words, characters or icons at said server computer to obtain extracted data and remainder data thereat,

separately storing said extracted data from said remainder data via server computer; and,

permitting reconstruction of said data via said extracted data and remainder data only in the presence of a predetermined security clearance via said server computer and as adapted to be downloaded to said client computer.

139. A method as claimed in claim 138 wherein said server computer utilizes at least two memory stores and the step of separately storing includes the step of said server computer separately storing said extracted data and said remainder data in respective ones of said two memory stores.

140. A method as claimed in claim 139 including storing a map of said two memory stores.

141. A method as claimed in claim 140 including encrypting at least one of said extracted data prior to storage, said remainder data prior to storage, and said map prior to storage.

142. A method as claimed in claim 141 wherein said map is stored via said server computer.

143. A method as claimed in claim 142 including the step of decrypting via said server computer said at least one of said extracted data prior to reconstruction, said remainder data prior to reconstruction, and said map prior to reconstruction.

144. A computer readable medium containing programming instructions for securing data in a computer system having at least a data input device, a processor and a memory with distributed segments, the programming instructions comprising:

establishing a group of security sensitive words or characters;

filtering data input from said data input device and extracting said security sensitive words or characters from said data to obtain extracted data and remainder data;

separately storing said extracted data and said remainder data in different distributed memory segments; and,

permitting reconstruction of said data via said extracted data and remainder data only in the presence of a predetermined security clearance.

145. A medium with programing instructions as claimed in claim 144 including establishing a plurality of security levels each with a respective security clearance, correlating said plurality of security levels with subsets of said security sensitive words, characters or icons and permitting reconstruction including the step of permitting a plurality of partial reconstructions of said data in the presence of respective ones of said plurality of security clearance levels.

146. A medium with programming instructions as claimed in claim 144 including encrypting one or both of said extracted data and remainder data.

147. A medium with programming instructions as claimed in claim 146 including encrypting during the filtering step and prior to the storing step.

148. A medium with programming instructions as claimed in claim 147 including decrypting during the reconstruction step.

149. A medium with programming instructions as claimed in claim 144 including one of destroying or storing said filter after the filtering step.

150. A medium with programming instructions as claimed in claim 144 including deleting said data input from said data input device after the step of storing.

151. A medium with programming instructions as claimed in claim 144 including mapping said different distributed memory segments.

152. A medium with programming instructions as claimed in claim 151 including mapping with encryption said different distributed memory segments.

153. A computer readable medium containing programming instructions for securing data in a computer network having a plurality of computers interconnected together, one of said plurality of computers designated as a data input computer and each of said plurality of computers having a memory therein, a first and a second memory designated as a remainder store and an extract store in one or more computers in said plurality of computers, the programming instructions comprising:

establishing a group of security sensitive words, characters or icons;

filtering data input from said data input computer and extracting said security sensitive words, characters or icons from said data to obtain extracted data and remainder data;

storing said extracted data and said remainder data in said extracted store and said remainder store, respectively; and,

permitting reconstruction of said data via said extracted data and remainder data only in the presence of a predetermined security clearance.

154. A medium with programing instructions as claimed in claim 153 including establishing a plurality of security levels each with a respective security clearance, correlating said plurality of security levels with subsets of said security sensitive words, characters or icons and permitting reconstruction including the step of permitting a plurality of partial reconstructions of said data in the presence of respective ones of said plurality of security clearance levels.

155. A medium with programming instructions as claimed in claim 153 including encrypting one or both of said extracted data and remainder data.

156. A medium with programming instructions as claimed in claim 155 including encrypting during the filtering step and prior to the storing step.

157. A medium with programming instructions as claimed in claim 156 including decrypting during the reconstruction step.

158. A medium with programming instructions as claimed in claim 153 including one of destroying or storing said filter after the filtering step.

159. A medium with programming instructions as claimed in claim 153 including deleting said data input from said data input computer after the step of storing.

160. A medium with programming instructions as claimed in claim 153 including mapping said first and second memory.

161. A computer readable medium containing programming instructions for securing data having a group of security sensitive words, characters or icons, the programming instructions utilized in conjunction with a client-server computer system with at least one server computer operatively coupled to at least one client computer over a communications network, the programming instructions comprising:

accepting data input which includes some words, characters or icons from said group of security sensitive words, characters or icons via said client computer;

filtering said data input and extracting said security sensitive words, characters or icons from said data to obtain extracted data and remainder data;

separately storing said extracted data from said remainder data in one or both of said client computer and server computer; and,

permitting reconstruction of said data via said extracted data and remainder data only in the presence of a predetermined security clearance on said client computer.

162. A medium with programming instructions as claimed in claim 161 wherein filtering occurs at one of said client computer and said server computer.

163. A medium with programming instructions as claimed in claim 161 wherein one or more of the filtering and separately storing occur at said server computer.

164. A medium with programming instructions as claimed in claim 161 wherein said server computer utilizes at least two memory stores and separately storing includes said server computer separately storing said extracted data and said remainder data in respective ones of said two memory stores.

165. A medium with programming instructions as claimed in claim 164 including storing a map of said two memory stores.

166. A medium with programming instructions as claimed in claim 165 including encrypting at least one of said extracted data prior to storage, said remainder data prior to storage, and said map prior to storage.

167. A medium with programming instructions as claimed in claim 166 wherein said map is stored on one of said client computer and said server computer.

168. A medium with programming instructions as claimed in claim 167 including decrypting said at least one of said extracted data prior to reconstruction, said remainder data prior to reconstruction, and said map prior to reconstruction.

169. A medium with programming instructions as claimed in claim 161 including establishing said group of security sensitive words, characters or icons.

170. A medium with programming instructions as claimed in claim 169 including establishing a plurality of security levels each with a respective security clearance, the step of establishing said security sensitive words, characters or icons including correlating said plurality of security levels with subsets of said security sensitive words, characters or icons and the step of permitting reconstruction including the step of permitting a plurality of partial reconstructions of said data in the presence of respective ones of said plurality of security clearance levels.

171. A medium with programming instructions as claimed in claim 161 including one of destroying or storing the filter after the filtering step.

172. A medium with programming instructions as claimed in claim 161 wherein said client-server computer system includes an output client computer having a display fed from video

memory having a plurality of frame memory segments, the reconstruction including interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments of said output client computer.

173. A medium with programming instructions as claimed in claim 161 wherein said client-server computer system includes an output client computer having a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces, the reconstruction including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays of said output client computer.

174. A medium with programming instructions as claimed in claim 161 including deleting said data input after storing.

175. A medium with programming instructions as claimed in claim 161 including mapping the storage of said extracted data and said remainder data in one or both of said client computer and said server computer.

176. An information processing system for securing data having one or more security sensitive words, characters or icons in a computer system, said computer system having at least a data input device, a processor and memory, all interconnected together, said memory having distributed memory segments, the information processing system comprising:

a filter adapted to receive data input from said data input device and to separate, from said data input, said security words, characters or icons, as extracted data, leaving remainder data;

a memory store, coupled to said filter, for storing said extracted data and said remainder data in separate distributed memory segments;

a security clearance control, coupled to said memory segments, enabling access to said memory segments; and

a compiler, coupled to said security control and said memory segments, for reconstructing said data input from said extracted data and said remainder data dependent upon access provided by said security clearance control.

177. An information processing system as claimed in claim 176 including a plurality of security levels each with a respective security clearance such that subsets of said security sensitive words, characters or icons correlate to said plurality of security levels, said security clearance control being responsive to said plurality of security levels, and said compiler providing a full reconstruction and a plurality of partial reconstructions of said data input dependent upon access provided by said security clearance control responsive to said plurality of security levels.

178. An information processing system as claimed in claim 176 including an encryptor coupled to said filter for encrypting one or both of said extracted data and remainder data.

179. An information processing system as claimed in claim 178 including a decryptor coupled to said compiler for decrypting one or both of said extracted data and remainder data prior to reconstruction of said data input.

180. An information processing system as claimed in claim 176 including means for deleting said filter, coupled to said filter.

181. An information processing system as claimed in claim 176 wherein said computer system includes a display fed from a video memory having a plurality of frame memory segments, the information processing system including said compiler adapted to be coupled to said video

memory and having means for interleaving said extracted data and remainder data into respective ones of said plurality of frame memory segments.

182. An information processing system as claimed in claim 176 wherein said computer system includes a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces, the information processing system including said compiler adapted to be coupled to said at least two respective display interfaces and having means for displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays.

183. An information processing system as claimed in claim 176 including means for deleting said data input from said data input device, coupled to said data input device.

184. An information processing system as claimed in claim 176 including means for mapping said separate distributed memory segments, coupled to said memory store.

185. An information processing system as claimed in claim 177 including an encryptor coupled to said filter for encrypting one or both of said extracted data and remainder data.

186. An information processing system as claimed in claim 185 including a decryptor coupled to said compiler for decrypting one or both of said extracted data and remainder data prior to reconstruction of said data input.

187. An information processing system as claimed in claim 186 including means for deleting said filter, coupled to said filter.

188. An information processing system as claimed in claim 187 wherein said computer system includes a display fed from a video memory having a plurality of frame memory segments, the information processing system including said compiler adapted to be coupled to said video

memory and having means for interleaving said extracted data and remainder data into respective ones of said plurality of frame memory segments.

189. An information processing system as claimed in claim 188 including means for deleting said data input from said data input device, coupled to said data input device.

190. An information processing system as claimed in claim 189 including means for mapping said separate distributed memory segments, coupled to said memory store.

191. An information processing system as claimed in claim 186 wherein said computer system includes a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces, the information processing system including said compiler adapted to be coupled to said at least two display interfaces and having means for displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays.

192. An information processing system as claimed in claim 191 including means for deleting said data input from said data input device, coupled to said data input device.

193. An information processing system as claimed in claim 192 including means for mapping said separate distributed memory segments, coupled to said memory store.

194. An information processing system as claimed in claim 193 including means for deleting said data input from said data input device, coupled to said data input device.

195. An information processing system as claimed in claim 194 including means for mapping said separate distributed memory segments, coupled to said memory store.

196. An information processing system as claimed in claim 176 wherein said computer system is a personal computer and said memory includes fixed drive memory, floppy drive memory

and removable disc drive memory, the information processing system including means for locating said distributed memory segments in one or more of said fixed drive memory, floppy drive memory and removable disc drive memory.

197. An information processing system as claimed in claim 195 wherein said computer system is a personal computer and said memory includes fixed drive memory, floppy drive memory and removable disc drive memory, the information processing system including means for locating said distributed memory segments in one or more of said fixed drive memory, floppy drive memory and removable disc drive memory.

198. An information processing system as claimed in claim 176 wherein said computer system includes a plurality of personal computers (PCs) networked together, each PC having distributed memory segments therein, the information processing system including means for storing, in said memory store, one or both of said extracted data and remainder data in said separate distributed memory segments of said PCs.

199. An information processing system as claimed in claim 195 wherein said computer system includes a plurality of personal computers (PCs) networked together, each PC having distributed memory segments therein, the information processing system including means for storing, in said memory store, one or both of said extracted data and remainder data in said separate distributed memory segments of said PCs.

200. An information processing system for securing data having one or more security sensitive words, characters or icons in a computer system, said computer system having at least a data input device, a processor and memory, all interconnected together, said memory having distributed segments, the information processing system comprising:

a filter, coupled to said data input device, adapted to be supplied with data input having at least one of said security sensitive words, characters or icons and obtaining extracted data and remainder data therefrom;

an extracted data store and a remainder data store, adapted to be defined in said distributed memory segments, said extracted data store and remainder data store accepting and storing said extracted data and remainder data from said filter; and,

a compiler, coupled to said extracted data store and remainder data store, for reconstructing said data input via said extracted data and remainder data only in the presence of a predetermined security clearance.

201. An information processing system as claimed in claim 200 including a plurality of security levels each with a respective security clearance such that subsets of said security sensitive words, characters or icons correlate to said plurality of security levels, said predetermined security clearance being responsive to said plurality of security levels, and said compiler providing a full reconstruction and a plurality of partial reconstructions of said data input dependent upon said predetermined security clearance as responsive to said security levels.

202. An information processing system as claimed in claim 200 including an encryptor coupled to said filter for encrypting one or both of said extracted data and remainder data.

203. An information processing system as claimed in claim 202 including a decryptor coupled to said compiler for decrypting one or both of said extracted data and remainder data for said reconstructing of said data input.

204. An information processing system as claimed in claim 200 including means for deleting said filter, coupled to said filter.

205. An information processing system as claimed in claim 200 wherein said computer system includes a display fed from video memory having a plurality of frame memory segments, the information processing system including said compiler adapted to be coupled to said video memory and having means for interleaving said extracted data and remainder data into respective ones of said plurality of frame memory segments.

206. An information processing system as claimed in claim 200 wherein said computer system includes a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces, the information processing system including a compiler adapted to be coupled to said at least two display interfaces and having means for displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays.

207. An information processing system as claimed in claim 200 including means for deleting said data input from said data input device, coupled to said data input device.

208. An information processing system as claimed in claim 200 including means for mapping said extracted data store and said remainder data store, coupled to said extracted data store and said remainder data store.

209. An information processing system as claimed in claim 201 including an encryptor coupled to said filter for encrypting one or both of said extracted data and remainder data.

210. An information processing system as claimed in claim 209 including a decryptor coupled to said compiler for decrypting one or both of said extracted data and remainder data for reconstruction of said data input.

211. An information processing system as claimed in claim 210 including means for deleting said filter, coupled to said filter.

212. An information processing system as claimed in claim 211 wherein said computer system includes a display fed from video memory having a plurality of frame memory segments, the information processing system including said compiler adapted to be coupled to said video memory and having means for interleaving said extracted data and remainder data into respective ones of said plurality of frame memory segments.

213. An information processing system as claimed in claim 212 including means for deleting said data input from said data input device, coupled to said data input device.

214. An information processing system as claimed in claim 213 including means for mapping said extracted data store and said remainder data store, coupled to said extracted data store and said remainder data store.

215. An information processing system as claimed in claim 211 wherein said computer system includes a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces, the information processing system including said compiler adapted to be coupled to said at least two display interfaces and having means for displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays.

216. An information processing system as claimed in claim 215 including means for deleting said data input from said data input device, coupled to said data input device.

217. An information processing system as claimed in claim 216 including means for mapping said extracted data store and said remainder data store, coupled to said extracted data store and said remainder data store.

218. An information processing system as claimed in claim 217 including means for deleting said data input from said data input device, coupled to said data input device.

219. An information processing system as claimed in claim 218 including means for mapping said extracted data store and said remainder data store, coupled to said extracted data store and said remainder data store.

220. An information processing system as claimed in claim 200 wherein said computer system is a personal computer and said memory includes fixed drive memory, floppy drive memory and removable disc drive memory, the information processing system including means for locating said distributed memory segments in one or more of said fixed drive memory, floppy drive memory and removable disc drive memory.

221. An information processing system as claimed in claim 219 wherein said computer system is a personal computer and said memory includes fixed drive memory, floppy drive memory and removable disc drive memory, the information processing system including means for locating said distributed memory segments in one or more of said fixed drive memory, floppy drive memory and removable disc drive memory.

222. An information processing system as claimed in claim 200 wherein said computer system includes a plurality of personal computers (PCs) networked together, each PC having distributed memory segments therein, the information processing system including means for storing,

in said extracted data store and said remainder data store, said extracted data and said remainder data in respective distributed memory segments of said PCs.

223. An information processing system as claimed in claim 219 wherein said computer system includes a plurality of personal computers (PCs) networked together, each PC having distributed memory segments therein, the information processing system including means for storing, in said extracted data store and said remainder data store, said extracted data and said remainder data in respective distributed memory segments of said PCs.

224. An information processing system for securing data having one or more security sensitive words, characters or icons in a computer network, said computer network having a plurality of computers interconnected together, one of said plurality of computers designated as a data input computer, each of said plurality of computers having a memory therein, said plurality of computers including a first and a second designated computer therein, the information processing system comprising:

a filter adapted to receive data input from said data input computer and to separate, from said data input, said security sensitive words, characters or icons, as extracted data, leaving remainder data;

a memory store, coupled to said filter, for storing said extracted data in said memory of said first designated computer and said remainder data in said memory of said second designated computer;

a security clearance control, coupled to said memory store of said first and second designated computers, controlling access to said memory store; and

a compiler, coupled to said security control and said memory store, for reconstructing said data input from said extracted data and said remainder data dependent upon access provided by said security clearance control.

225. An information processing system as claimed in claim 224 including means for mapping said memory of said first and second designated computers, coupled to said memory store.

226. An information processing system as claimed in claim 225 wherein said means for mapping creates a map to locate said memory store, the system including a map store, coupled to said means for mapping, for storing said map.

227. An information processing system as claimed in claim 226 including an encryptor coupled to said filter for encrypting said map and a decryptor coupled to said compiler for decrypting said map.

228. An information processing system as claimed in claim 224 wherein said second computer is said data input computer and said filter is adapted to be coupled to said second computer.

229. An information processing system as claimed in claim 224 including an encryptor coupled to said filter for encrypting one or both of said extracted data and remainder data.

230. An information processing system as claimed in claim 229 including a decryptor coupled to said compiler for decrypting one or both of said extracted data and remainder data.

231. An information processing system as claimed in claim 224 including means for deleting said filter, coupled to said filter.

232. An information processing system as claimed in claim 224 wherein one of said computers includes a display fed from a video memory having a plurality of frame memory

segments, the information processing system including said compiler adapted to be coupled to said video memory, said compiler having means for interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments on said one computer.

233. An information processing system as claimed in claim 224 wherein one of said computers includes a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces, the information processing system including said compiler adapted to be coupled to said at least two display interfaces, said compiler having means for displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays on said one computer.

234. An information processing system as claimed in claim 224 including means for deleting said data input from said data input computer, coupled to said data input device.

235. An information processing system for securing data from a data input having one or more security sensitive words, characters or icons, the information processing system operative in a client-server computer system with at least one server computer operatively coupled to at least one client computer over a communications network, said information processing system comprising:

a filter adapted to receive said data input from said communications network and to separate, from said data input, said security sensitive words, characters or icons as extracted data, leaving remainder data;

at least one memory store, coupled to said filter, for separately storing said extracted data and said remainder data in one or both of said client computer and server computer;

a compiler, coupled to said at least one memory store, for reconstructing said data input via said extracted data and remainder data only in the presence of a predetermined security clearance on said client computer.

236. An information processing system as claimed in claim 235 wherein said filter is disposed at one of said client computer and said server computer.

237. An information processing system as claimed in claim 235 wherein said filter is disposed at said server computer and said memory store separately stores one of said extracted data and said remainder data at said server computer.

238. An information processing system as claimed in claim 235 wherein said server computer utilizes at least two memory stores and the server memory stores separately store said extracted data and said remainder data.

239. An information processing system as claimed in claim 238 including means for mapping said server stores, said means for mapping adapted to be coupled to said at least one server computer.

240. An information processing system as claimed in claim 239 wherein said means for mapping creates a map to said server stores and further the system includes means for storing said map in one of said at least one client computer and said at least one server computer.

241. An information processing system as claimed in claim 240 including an encryptor coupled to said filter for encrypting at least one of said extracted data, said remainder data, and said map.

242. An information processing system as claimed in claim 241 including a decryptor coupled to said filter for decrypting at least one of said extracted data, said remainder data, and said map.

243. An information processing system as claimed in claim 235 including a database adapted to be coupled to one of said client computer and said server computer for said security sensitive words, characters or icons, said database coupled to said filter.

244. An information processing system as claimed in claim 243 including a plurality of security levels each with a respective security clearance such that subsets of said security sensitive words, characters or icons correlate to said plurality of security levels, said predetermined security clearance being dependent upon said plurality of security levels, and said compiler providing a full reconstruction and a plurality of partial reconstructions of said data input in the presence of respective ones of said plurality of security clearance levels.

245. An information processing system as claimed in claim 235 including means for deleting said filter, coupled to said filter.

246. An information processing system as claimed in claim 235 wherein said client-server computer system includes an output client computer having a display fed from a video memory having a plurality of frame memory segments, the information processing system including said compiler adapted to be coupled to said video memory and said compiler having means for interleaving said extracted data and remainder data into respective ones of said plurality of frame memory segments of said output client computer.

247. An information processing system as claimed in claim 235 wherein said client-server computer system includes an output client computer having a data display system with at least two

separate but visually overlaid displays and at least two respective display interfaces, the information processing system including said compiler adapted to be coupled to said at least two display interfaces and said compiler having means for displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays of said output client computer.

248. An information processing system as claimed in claim 235 including means for deleting said data input, coupled to said at least one client computer.

249. An information processing system as claimed in claim 235 including means for mapping the storage of said extracted data and said remainder data in one or both of said client computer and said server computer.

250. An information processing system for securing data having a group of security sensitive words, characters or icons, said information processing system operative on a server-client computer system with at least one server computer operatively coupled to at least one client computer over a communications network, said client computer accepting data input which includes some words, characters or icons from said group of security sensitive words, characters or icons, and filtering said data input and extracting said security sensitive words, characters or icons from said data to obtain extracted data and remainder data thereat, said information processing system comprising:

at least one memory store adapted to be coupled to said at least one server computer for separately storing said extracted data from said remainder data via said at least one server computer; and,

a compiler coupled to said at least one memory store for reconstructing said data input via said extracted data and remainder data only in the presence of a predetermined security clearance via said at least one server computer and as adapted to be downloaded to said at least one client computer.

251. An information processing system as claimed in claim 250 wherein said at least one server computer includes at least two memory stores and said two memory stores separately store said extracted data and said remainder data in respective ones of said at least two memory stores.

252. An information processing system as claimed in claim 251 including means for creating a map of said at least two memory stores, coupled to said two memory stores.

253. An information processing system as claimed in claim 252 including an encryptor adapted to be coupled to said at least one client computer, for encrypting at least one of said extracted data, said remainder data, and said map.

254. An information processing system as claimed in claim 253 wherein said map is stored via said server computer.

255. An information processing system as claimed in claim 253 including a decryptor coupled to said compiler and said at least one memory store for decrypting via said at least one server computer said at least one of said extracted data, said remainder data, and said map.

256. An information processing system for securing data having a group of security sensitive words, characters or icons, said information processing system adapted to operate in a server-client computer system with at least one server computer operatively coupled to at least one client computer over a communications network, said client computer accepting data input which

includes some words, characters or icons from said group of security sensitive words, characters or icons, the information processing system comprising:

a filter adapted to receive data input from said at least one client computer and to separate at said at least one server computer from said data input said security sensitive words, characters or icons, as extracted data, leaving remainder data;

at least one memory store, coupled to said filter, for separately storing said extracted data from said remainder data via said at least one server computer; and,

a compiler, coupled to said at least one memory store, for reconstructing of said data input via said extracted data and remainder data only in the presence of a predetermined security clearance via said at least one server computer and as adapted to be downloaded to said at least one client computer.

257. An information processing system as claimed in claim 256 wherein said at least one server computer includes at least two memory stores and said two memory stores separate store said extracted data and said remainder data in respective ones of said two memory stores.

258. An information processing system as claimed in claim 257 including means for creating a map of said at least two memory stores, coupled to said at least two memory stores.

259. An information processing system as claimed in claim 258 including an encryptor, coupled to said filter, for encrypting at least one of said extracted data, said remainder data, and said map.

260. An information processing system as claimed in claim 259 wherein said map is stored via said at least one server computer.

261. An information processing system as claimed in claim 260 including a decryptor coupled to said compiler for decrypting via said at least one server computer said at least one of said extracted data, said remainder data, and said map.

262. An information processing system for securing data in a computer system having at least a data input device, a processor and memory, all interconnected together, said memory having distributed segments, comprising:

means for establishing a group of security sensitive words, characters or icons;

a filter, coupled to said data input device and said means for establishing, extracting said security sensitive words, characters or icons from data input from said data input device and obtaining extracted data and remainder data;

an extracted data store and a remainder data store defined in said distributed memory segments and accepting said extracted data and remainder data from said filter; and,

compiler, coupled to said extracted data store and a remainder data store, for reconstructing said data via said extracted data and remainder data only in the presence of a predetermined security clearance.